

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-045212

(43)Date of publication of application : 16.02.1999

(51)Int.Cl.

G06F 12/14

(21)Application number : 09-217025

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 29.07.1997

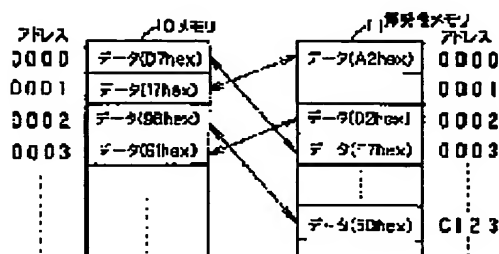
(72)Inventor : NARASHIMA TAKAAKI

## (54) OPPOSING METHOD AGAINST DECIPHERING ATTACK REGARDING SECRET INFORMATION

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To oppose an attack for deciphering secret information by replacing and storing the secret information in a different place by electronic devices each time it is written to a volatile memory.

**SOLUTION:** Data on the address 0000 of secret information before conversion in a memory 10 are D7hex and when the secret information is stored for the first time according to a storage converting rule, it is stored in address 0003 of the volatile memory 11 by conversion to F7hex. For second storage, it is stored in address 0003 of the volatile memory 11 by conversion to code data other than F7hex. Similarly, data on the address 0001 are 17hex, first storage in the address 0003 of the volatile memory 11 is performed by conversion to A2hex, and data on the address 0002 are 9Bhex; and first storage in address C123 of the volatile memory 11 is performed by conversion to 5Dhex. Thus, the secret information is stored in different places by electronic devices each time it is stored in the memory.



## LEGAL STATUS

[Date of request for examination] 27.06.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-45212

(43) 公開日 平成11年(1999) 2月16日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

3 2 0 B

3 2 0 D

審査請求 未請求 請求項の数 3 F D (全 5 頁)

(21) 出願番号 特願平9-217025

(22) 出願日 平成9年(1997) 7月29日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 楢島 高明

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

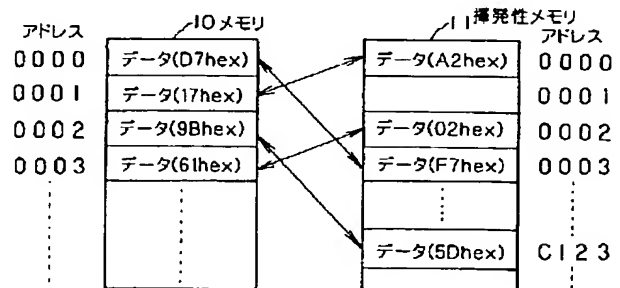
(74) 代理人 弁理士 青木 輝夫

(54) 【発明の名称】 秘密情報の解読攻撃対抗方法

(57) 【要約】

【課題】 揮発性メモリに秘密情報を書き込む場合に該秘密情報の内容及び格納位置を変換することにより、秘密情報の解読の攻撃に対抗する。

【解決手段】 変換後の秘密情報を格納する揮発性メモリ11を有する秘密情報の解読攻撃対抗方法において、書き込み時に情報を任意に変換する手段を具備し、この変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納する。



1

## 【特許請求の範囲】

【請求項 1】 秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納することを特徴とする秘密情報の解読攻撃対抗方法。

【請求項 2】 変換手段は、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えを行うスイッチで構成され、該スイッチにより前記アドレス信号線及びデータ信号線任意に入れ替えられることを特徴とする請求項 1 記載の秘密情報の解読攻撃対抗方法。

【請求項 3】 変換手段は、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えるための情報が書き込まれる変換用メモリで構成され、該変換用メモリの情報により非線形に秘密情報が格納させることを特徴とする請求項 1 記載の秘密情報の解読攻撃対抗方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、筐体に収納された電子機器のメモリに保持されている秘密情報を解読しようとする攻撃に対抗する方法に関するものである。

【0002】

【従来の技術】従来から秘密情報を保持した電子機器には、電子機器の筐体を分解し保持されている秘密情報をメモリから容易に読み出され解読されないようにする種々の方法が施されている。例えば、電子機器内部の揮発性メモリに格納された秘密情報を解読しようとする攻撃に対抗 (Tamper Resistant) する方法として、メモリを容器に封入し外部からの攻撃を検知する手段を具備し、攻撃を受けるとメモリ内部の秘密情報を消去する方法が特開平 2 - 4 4 4 4 7 号公報等で知られている。

【0003】

【発明が解決しようとする課題】しかしながら、上記のような従来の攻撃を検知してメモリ内部の秘密情報を消去する方法では、その消去する構造が解明されてしまうとバックアップされた揮発性メモリの秘密情報を消去せずに読み取ることが可能になる。例えば、複数の読み取られた情報の内容比較や情報が収納されている位置関係から解読する条件を与えるという問題がある。

【0004】本発明は、上記のような問題を解決するものであり、揮発性メモリに秘密情報を書き込む場合に該秘密情報の内容及び格納位置を変換することにより、秘密情報の解読の攻撃に対抗できるようにした秘密情報の解読攻撃対抗方法を提供することを目的とする。

【0005】

【課題を解決するための手段】上記課題を解決するために本発明は、秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記

2

変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納することを特徴とする。

【0006】本発明によれば、秘密情報の解読の攻撃に対抗できる。

【0007】

【発明の実施の形態】本発明の請求項 1 に記載の発明は、秘密情報を保持する揮発性メモリに対して、書き込み情報を任意に変換する手段を具備し、前記変換手段により秘密情報を電子機器毎及び揮発性メモリに書き込む毎に異なる場所に変換して格納するものであり、揮発性メモリに書き込まれた秘密情報の位置が不特定となることにより、複数の読み出された秘密情報から解読の手がかりとなる情報を与えにくくすることができるという作用を有する。

【0008】請求項 2 に記載の発明は、変換手段が、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えを行うスイッチで構成され、該スイッチにより前記アドレス信号線及びデータ信号線任意に入れ替えられるものであり、アドレス及びデータの信号線数に対応した任意のアドレス順とデータのビット位置を入れ替えてアクセスすることができ、同じ秘密情報を各装置に書き込んでもメモリ上の情報は信号線の組み合わせ数まで装置単位で異なるようにすることができるという作用を有する。

【0009】請求項 3 に記載の発明は、変換手段が、アドレス信号線及びデータ信号線の情報を任意に変換して各信号線の入れ替えるための情報が書き込まれる変換用メモリで構成され、該変換用メモリの情報により非線形に秘密情報が格納させるものであり、揮発性メモリに対して非線形の空間に秘密情報を格納することができ、かつ信号線の組み合わせ以上に変換して揮発性メモリをアクセスすることができるという作用を有する。

【0010】以下、本発明の実施の形態について、図 1 ～図 5 を用いて説明する。

【0011】（実施の形態 1）図 1 は、本発明の実施の形態 1 における秘密情報の解読攻撃対抗方法により秘密情報を揮発性メモリに任意の場所に情報を変換して格納する場合の原理説明図である。図 1 において、10 は変換される以前の秘密情報の格納状態を表したメモリであり、11 は電子機器毎及びメモリに書き込む毎に異なる格納変換法則に基づいて秘密情報を格納した後の状態を表す揮発性メモリである。

【0012】この構成において、メモリ 10 における変換以前の秘密情報のアドレス 0000 番地のデータは D7 hex であり、この秘密情報の格納変換法則に基づく 1 回目の格納は、揮発性メモリ 11 のアドレス 0003 番地に F7 hex と変換されて格納される。また、2 回目の格納は、揮発性メモリ 11 のアドレス 0003 番地に F7 hex 以外のコードデータに変換して格納され

3

る。

【0013】以下同様にして、メモリ10における変換以前の秘密情報のアドレス0001番地のデータは17hexであり、この秘密情報の格納変換法則に基づく1回目の格納は、揮発性メモリ11のアドレス0003番地にA2hexと変換されて格納され、また、メモリ10における変換以前の秘密情報のアドレス0002番地のデータは9Bhexであり、この秘密情報の格納変換法則に基づく1回目の格納は、揮発性メモリ11のアドレスC123番地に5Dhexと変換されて格納される。同様に、2回目の格納は、上記アドレス番地に上記以外のコードデータに変換して格納されることになる。また、揮発性メモリ11に変換されて格納されている秘密情報を読み出す時は、格納時と逆の変換を行うことによりメモリ10に示す変換以前の秘密情報に戻すことができる。

【0014】このように電子機器毎及びメモリに書き込む毎に異なる場所に格納変換法則に基づき秘密情報を情報変換して揮発性メモリに格納するため、この揮発性メモリに格納された秘密情報を複数に亘り読み出して比較したとしても、解読するための特徴を解り難くすることが可能になる。

【0015】（実施の形態2）図2～図4により本発明の実施の形態2について説明する。図2は実施の形態1の方法を、揮発性メモリとマイクロプロセッサ間を接続するアドレスバスとデータバスに変換回路を設けることで実現するようにしたブロック図であり、図3は変換回路を切替スイッチにより構成した場合のブロック図であり、図4は切替スイッチの構成図である。

【0016】図2において、12はマイクロプロセッサ(MPU)、13はマイクロプロセッサ12の制御下で電子機器の外部から転送されてきた秘密情報を電子機器毎及びメモリに書き込む毎に異なる場所に格納変換法則に基づき変換する変換回路、14は変換回路13で変換された秘密情報を格納する揮発性メモリである。マイクロプロセッサ12と変換回路13間はアドレスバス15とデータバス16により接続され、変換回路13と揮発性メモリ14間はアドレスバス17とデータバス18により接続されている。

【0017】図3において、変換回路13は、マイクロプロセッサ12のアドレス端子A0～An及びデータ端子D0～Dmに対応する数の1:nのセレクトタイプのアドレス用切替スイッチSWA0、SWA1・・・及び1:mのセレクトタイプのデータ用切替スイッチSWD0、SWD1・・・から構成され、各アドレス用切替スイッチSWA0、SWA1・・・の1入出力端はマイクロプロセッサ12のアドレスA0～Anのアドレス信号線に接続され、さらに、各アドレス用切替スイッチSWA0、SWA1・・・のn入出力端の同じ信号線は揮発性メモリ14のアドレスA0～Anのアドレス信号線に

4

並列に接続されている。また、データ用切替スイッチSWD0、SWD1・・・の1入出力端はマイクロプロセッサ12のデータD0～Dmのデータ信号線に接続され、さらに、各データ用切替スイッチSWD0、SWD1・・・のn入出力端の同じ信号線は揮発性メモリ14のデータD0～Dmのデータ信号線に並列に接続されている。

【0018】図4はアドレス用及びデータ用切替スイッチの構成を示すもので、1:nまたは1:mのセレクトタイプのスイッチから構成され、この切替スイッチはマイクロプロセッサ12からの制御信号SWSELxxにより切替部SWxxをnまたはmの入出力B、C、D・・・に切り替えることで、入出力Aをnまたはmの入出力B、C、D・・・に切り替えるようになっている。

【0019】上記の構成において、各切替スイッチの入出力B以降は同じ信号線同志で接続され、また、各切替スイッチはマイクロプロセッサ12からの制御信号によりアドレスバス単位及びデータバス単位で同じ信号線が選択されるように制御されるから、例えば、切替スイッチSWA0入出力Aは、マイクロプロセッサ12のアドレスA0に接続され、切替スイッチSWA0の入出力B以降は揮発性メモリ14のアドレスA0～Anに接続される。そして、マイクロプロセッサ12からの制御信号SWSELxxにより、揮発性メモリ14のアドレスA1が選択されているとすれば、切替スイッチSWA0以外の切替スイッチは揮発性メモリ14のアドレスA1以外のアドレスが選択されることになる。また、データの場合もアドレスの場合と同様にして変換できる。

【0020】従って、このような本実施の形態2によれば、マイクロプロセッサ12のソフトウェアからは、同一のメモリ空間に見え、しかも不連続な任意のアドレス空間にデータを格納でき、かつ格納されたデータのビット位置の変えることができるから、同じ秘密情報を各電子機器に書き込んでもメモリ上の情報は信号線の組み合わせ数まで装置単位で異なるようすることができる。

【0021】（実施の形態3）図5により本発明の実施の形態3について説明する。図5は変換回路13に変換メモリを使用した場合の構成を示すブロック図である。

【0022】図5において、変換回路13は、アドレスを変換するための情報を書き込んだアドレス変換用メモリ131、データを書き込む時に変換するための情報を書き込んだデータ書き込み変換用メモリ132、データを読み込む時に変換するための情報を書き込んだデータ読み込み変換用メモリ133、及びデータを書き込む時とデータを読み込む時にデータバスを切り替えることによりデータ書き込み変換用メモリ132またはデータ読み込み変換用メモリ133を選択するデータバス切替器134、135を備える。

【0023】上記の構成において、揮発性メモリ14をアクセスするマイクロプロセッサ12のアドレスはアド

5

レス変換用メモリ 1 3 1 により変換され、この変換されたアドレスを揮発性メモリ 1 4 に出力することにより、揮発性メモリ 1 4 は図 1 に示すように非線形にアクセスされることになる。また、秘密情報の書き込み時は、マイクロプロセッサ 1 2 のデータバスがデータバス切替器 1 3 4 によりデータ書き込み変換用メモリ 1 3 2 のアドレスバスに接続され、かつデータ書き込み変換用メモリ 1 3 2 のデータバスはデータバス切替器 1 3 5 により揮発性メモリ 1 4 のデータバスに接続される。また、秘密情報の読み込み時は、揮発性メモリ 1 4 のデータバスがデータバス切替器 1 3 5 によりデータ読み込み変換用メモリ 1 3 3 のアドレスバスに接続され、かつデータ読み込み変換用メモリ 1 3 3 のデータバスはデータバス切替器 1 3 4 によりマイクロプロセッサ 1 2 のデータバスに接続される。

【0 0 2 4】従って、それぞれの変換用メモリ 1 3 1、1 3 2、1 3 3 に非線形になるような情報を書き込んでおくことにより、アドレス及びデータの信号線の組み合わせ以上に変換してアクセスすることができる。

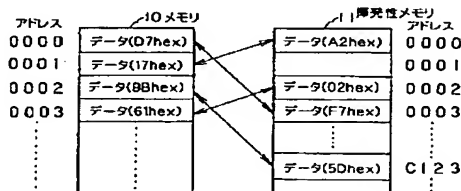
【0 0 2 5】

【発明の効果】以上のように本発明によれば、揮発性メモリに書き込まれた秘密情報の位置が不特定となることにより、複数の読み出された秘密情報から解読の手がかりとなる情報を与えにくくすることができる。

【0 0 2 6】また本発明によれば、アドレス信号線及びデータ信号線の情報を任意に変換する手段をスイッチで構成することにより、アドレス及びデータの信号線数に対応した任意のアドレス順とデータのビット位置を入れ替えてアクセスすることができ、このため、同じ秘密情報を各装置に書き込んでもメモリ上の情報は信号線の組

【0 0 2 7】また本発明によれば、アドレス信号線及び

【図 1】



6

データ信号線の情報を任意に変換するための情報を書き込んだ変換用メモリの情報により、揮発性メモリに対して非線形の空間に秘密情報を格納することができ、かつ信号線の組み合わせ以上に変換して揮発性メモリをアクセスすることができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態 1 における秘密情報の解読攻撃対抗方法により秘密情報を揮発性メモリに任意の場所に情報を変換して格納する場合の原理説明図

【図 2】本発明における実施の形態 1 の方法を、揮発性メモリとマイクロプロセッサ間を接続するアドレスバスとデータバスに変換回路を設けることで実現するようにした実施の形態 2 のブロック図

【図 3】本発明の実施の形態 2 における変換回路を切替スイッチにより構成した場合のブロック図

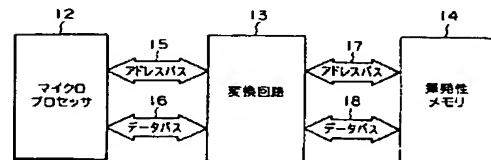
【図 4】本発明の実施の形態 2 における切替スイッチの構成図

【図 5】本発明の実施の形態 3 において変換回路に変換メモリを使用した場合の構成を示すブロック図

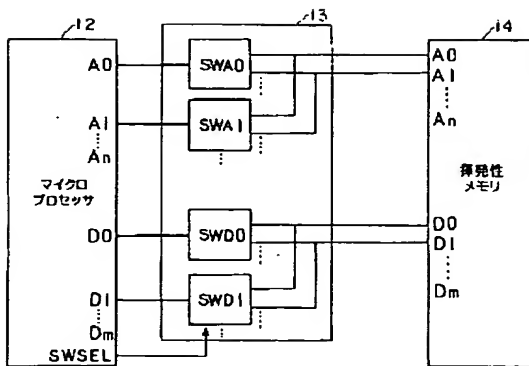
【符号の説明】

- 1 0 変換以前の秘密情報の格納状態を表すメモリ
- 1 1 変換後の秘密情報の格納状態を表す揮発性メモリ
- 1 2 マイクロプロセッサ
- 1 3 変換回路
- 1 4 揮発性メモリ
- 1 5 、 1 7 アドレスバス
- 1 6、 1 8 データバス
- SWA 0、 SWA 1 アドレス用切替スイッチ
- SWD 0、 SWD 1 データ用切替スイッチ
- 1 3 1 アドレス変換用メモリ
- 1 3 2 データ書き込み変換用メモリ
- 1 3 3 データ読み込み変換用メモリ
- 1 3 4、 1 3 5 データバス切替器

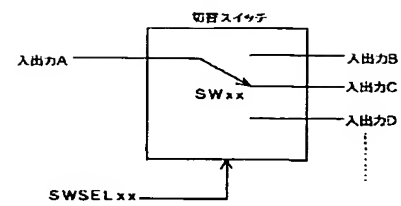
【図 2】



【図 3】



【図 4】



【図 5】

